lavery
Lawyers

Artificial Intelligence and Telework: Security Measures to be Taken

September 18, 2020

Author

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Cybersecurity will generally be a significant issue for businesses in the years to come. With teleworking, cloud computing and the advent of artificial intelligence, large amounts of data are likely to fall prey to hackers attracted by the personal information or trade secrets contained therein.

From a legal standpoint, businesses have a duty to take reasonable steps to protect the personal information they hold.[1] Although the legal framework doesn't always specify what such reasonable means are in terms of technology, measures appropriate for the personal information in question must nevertheless be applied. These measures must also be assessed in light of the evolution of threats to IT systems.

Some jurisdictions, such as Europe, go further and require that IT solutions incorporate security measures by design.[2] In the United States, with respect to medical information, there are numerous guidelines on the technical means to be adopted to ensure that such information is kept secure.[3]

In addition to the personal information they hold, companies may also want to protect their trade secrets. These are often invaluable and their disclosure to competitors could cause them irreparable harm.

No technology is immune. In a recent publication,[4] the renowned Kaspersky firm warns us of the growing risks posed by certain organized hacker groups that may want to exploit the weaknesses of Linux operating systems, despite their reputation as highly secure. Kaspersky lists a number of known vulnerabilities that can be used for ransom attacks or to gain access to privileged information. The publication echoes the warnings issued by the FBI regarding the discovery of new malware targeting Linux.[5]

Measures to be taken to manage the risk

It is thus important to take appropriate measures to reduce these risks. We recommended in particular that business directors and officers:

Adopt corporate policies that prevent the installation of unsafe software by users;
Adopt policies for the regular review and updating of IT security measures;
Have penetration tests and audits conducted to check system security;
Ensure that at least one person in management is responsible for IT security.

Should an intrusion occur, or, as a precautionary measure for businesses that collect and store sensitive personal information, consulting a lawyer specializing in personal information or trade secrets is recommended in order to fully understand the legal issues involved in such matters.

---

1. See in particular: *Act respecting the protection of personal information in the private sector* (Quebec), s. 10, *Personal Information Protection and Electronic Documents Act* (Canada), s. 3.
2. *General Data Protection Regulation*, art. 25.
3. *Security Rule, under the Health Insurance Portability and Accountability Act*, 45 CFR Part 160, 164.
4. https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
5. https://www.fbi.gov/news/pressrel/press-releases/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecurity-advisory